Westinghouse

INFORMATION SYSTEMS

BMS #: BMS-IS-54
Revision: 0.0
Effective Date: 10/31/2018

Acceptable Use of Technology Policy

Approval

Preparer:

______________________________ / ________
James S. Ringold Date
Chief Information Security Officer, IS

Owner:

Electronically Approved* / ________
James S. Ringold Date
Chief Information Security Officer, IS

Approver:

Electronically Approved* / ________
Yexi Liu Date
Westinghouse Chief Information Officer

*Electronically approved records are authenticated in the Business Management System (BMS).

*** This record was final approved on 3/16/2021 9:51:17 AM. (This statement was added by the PRIME system upon its validation)

Table of Contents

Purpose

The Acceptable Use of Technology policy supplements the Global Information Security Policy by establishing the user requirements for and prohibited uses of information resources, including computers, mobile devices, printers, removable storage, electronic messaging, and Internet services.

Scope

This policy applies to all employees, contingent labor personnel, vendors, business partners, customers and other third parties at all global locations and includes all Westinghouse computer systems or electronic devices (desktop, laptop, scanners, smartphones, tablet, or any other data processing device) owned, leased, operated, or maintained by or on behalf of Westinghouse.

Standard Approval and Review Process

This policy must be reviewed and approved in accordance with **BMS-CI-2: BMS Policy and Procedure**.

Policy

1.1 Personally Owned Computers and Mobile Devices

1.1.1 Users may access Westinghouse's Internet-accessible webmail and Citrix servers from personally owned computers and mobile devices.

1.1.2 The use of personally-owned computers or mobile devices to access networks, systems and data to perform work for Westinghouse or Westinghouse customers is prohibited. Westinghouse computer systems and computer data may only be accessed by and stored on Westinghouse computers, laptops, and mobile devices configured with approved Westinghouse IT security controls

1.1.3 Users are prohibited from bringing personally owned computers onto Westinghouse sites or Westinghouse customer sites.

1.2 Westinghouse Owned Computers

1.2.1 Users must protect Westinghouse computer systems from unauthorized access, damage, theft, loss, and illegal activity.

1.2.2 Users must immediately report the loss or theft of any Westinghouse computer or mobile device to the Westinghouse Service Desk.

1.2.3 Users must report device problems and deficiencies to the Westinghouse Service Desk.

1.2.4 In regards to Westinghouse computers users are prohibited from the following:

- Using the computer or device for non-business purposes;
- Intentionally damaging the computer;
- Installing non-standard software on the computer without first obtaining approval from Information Technology in accordance with **BMS-IS-11: Software Acquisition Policy**;
- Lending, falsifying, or misusing the computer or mobile device;

- Using another users login credentials to obtain access;
- Harassing or threatening another individual or persons;
- Copyright infringement or violating software agreements; and
- Making unauthorized configuration changes to the computer.

1.3 Westinghouse Owned Mobile Device Policy

Mobile devices include laptop computers, tablet computers, iPads, mobile phones, or similar devices capable of processing, transmitting, or storing information.

1.3.1 Only mobile devices approved and issued by the Westinghouse IT Department are permitted to access networks, systems and data used to perform Westinghouse business.

1.3.2 Westinghouse mobile devices may not be used for commercial activities that are not related to Westinghouse. Limited personal use is acceptable if it does not conflict with Westinghouse policies or usage limitations.

1.3.3 Mobile devices not owned by Westinghouse are not permitted to connect to either Westinghouse internal computer networks or customer internal computer networks. Connections to networks deemed for “guest” use may be permitted.

1.3.4 Westinghouse data may only be transmitted to, from, or stored on Westinghouse-owned mobile devices.

1.3.5 Westinghouse and customer data stored on mobile devices must be stored encrypted using Westinghouse-approved encryption products and technologies.

1.3.6 The loss or theft of any Westinghouse mobile device must be reported to the Westinghouse Service Desk immediately, who will then escalate the loss report to the Information Security Team and will also take appropriate action to disable the device and remove data from the device. In the event of theft, a police report must be obtained.

1.3.7 Westinghouse mobile devices will be securely configured in accordance to Westinghouse security standards described in the Westinghouse Computer Security Standard 204: *Workstations, Laptops, and Mobile Devices*.

1.3.8 The use of network, wireless, and cellular wireless services on Westinghouse mobile devices must comply with **Access to Networks and Network Services** of the BMS-IS-46 policy.

1.3.9 Westinghouse mobile devices used for development or delivery of customer designated digital products or services must comply with W2-9.17-102: *Westinghouse Portable Media and Mobile Device (PMMD) Program Procedure*

1.3.10 Westinghouse mobile devices and Westinghouse cellular services may be used on Westinghouse computers to connect to the Internet, as well as establish remote VPN connections, as long as the Westinghouse computer is in compliance with Westinghouse policies and standards and the Westinghouse computer is not simultaneously connected to the Westinghouse network and the user is working from a remote (non-Westinghouse) location.

1.4 Visitor Computers and Mobile Devices

1.4.1 Non-Westinghouse employees and contract labor personnel may bring visitor computer and mobile devices (i.e., computers and mobile devices owned by another organization) to Westinghouse facilities that permit them, but only under the following conditions:

- The Westinghouse facility permits non-Westinghouse devices;
- The non-Westinghouse device is configured, maintained, and owned by the visitors business organization;
- Prior written approval has been obtained from the visitor’s Westinghouse sponsor permitting the device at the Westinghouse facility;
- The device is declared to Corporate Security at visitor registration; and
- The visitor agrees in writing to comply with Westinghouse Computer Security Policies.

1.4.2 Visitor computers and mobile devices are prohibited from connecting to the Westinghouse company network.

1.4.3 Visitor computers and mobile devices may connect to the Westinghouse visitor network service.

1.5 Westinghouse Partner Computers and Mobile Devices

1.5.1 Westinghouse partner workstations are intended for the use of its partners to perform Westinghouse-approved work and to collaborate with Westinghouse personnel at Westinghouse facilities. Partner workstations will be managed using security controls and practices that protect the availability, confidentiality, and integrity of Westinghouse computer data.

1.5.2 Westinghouse partner workstations will not be configured to access internal Westinghouse network resources, including W-Intra resources. Westinghouse partner workstations will only access W-Partner domain resources. W-Intra domain users and resources, however, may access W-Partner domain resources.

1.5.3 Westinghouse partner workstations may access Internet resources unless compliance or security requirements prohibit this access.

1.5.4 Westinghouse partners will use a desktop workstation. Laptops and mobile devices are not permitted to be used as a Westinghouse partner computer.

1.5.5 Westinghouse partner workstations will not be removed from any Westinghouse facility nor used outside of any Westinghouse facility.

1.5.6 Westinghouse partner workstations will be physically secured using a cable lock or other means of physical security to prevent unauthorized relocation.

1.5.7 Westinghouse partners are prohibited from installing software on their Westinghouse partner workstation. Software that has been approved by the partner's sponsor and by Westinghouse Legal may be installed, but only by Information Technology using a W-Partner administrator account.

1.5.8 Westinghouse partner workstations will only print to printers designated as acceptable for use by Westinghouse partners. Printers that are not allowed include those in areas where partners are not permitted or where confidential Westinghouse internal documents are printed.

1.5.9 The use of document scanners or other imaging equipment by Westinghouse partners or visitors on premise at a Westinghouse location is prohibited.

1.6 Westinghouse Printers

1.6.1 Only approved printer models located in the Service Request list are authorized for purchase.

1.6.2 Printers with wireless capabilities are prohibited from being ordered.

1.6.3 Westinghouse printers are prohibited from being used connected using wireless connectivity and must only be connected using a physical connection such as USB, serial, or parallel port.

1.6.4 Westinghouse employees and visitors are prohibited from sharing local printers through the network.

1.7 Removable Media

1.7.1 Media Handling

- Removable media used to store or transfer Westinghouse electronic information, data, or files must be owned by Westinghouse with authorized encryption configured.
- Westinghouse electronic information, data, and files on removable media must be encrypted in accordance with BMS-IS-22 Westinghouse Computer Security Standard 232: *Encryption and Digital Certificates*.
- Users must immediately report the loss or theft of any removable storage devices to the Westinghouse Service Desk.
- Visitors or third parties wishing to transmit files between a non-Westinghouse portable memory storage device and a Westinghouse computer will provide the device to Information Technology. The memory stick will be checked for viruses and the files will be transferred from the stick to a location where they can be securely retrieved. The transfer will be approved in writing by a Westinghouse manager. Visitors or third parties are otherwise prohibited from bringing and using portable memory storage devices while at a Westinghouse site. Visitors found with portable memory storage devices will have these devices confiscated for inspection by Westinghouse.
- Visitors, vendors, or other third parties needing to transfer files to Westinghouse must declare the portable storage device in

advance of the visit through their Westinghouse host. The Westinghouse host must contact the Westinghouse IT Service Desk to have the Westinghouse IT Department determine if an alternate transfer method should be used, or if the removable media device may be presented upon arrival for inspection for malicious software and departure for proprietary information.

- Storage of Westinghouse electronic information, data, and files on removable media must comply with BMS-LGL-28 and BMS-LGL-32.
- All files accessed from removable media must be automatically scanned for malicious code at time of access.
- When removable media is required to be used for the development, test, or delivery of customer-designated digital products and services to Westinghouse customers, such removable media must be used in compliance with W2-9.17-102.

1.7.1 Disposal of Media

- Removable media destruction must be performed securely using a method approved by the Westinghouse Information Security Team.
- Persons who have media which needs to be securely destroyed should open an IT Service Desk Ticket to the Information Security Team.

1.7.2 Media Transfer

- The transfer of large files to third parties must be performed using the Westinghouse Large File Transfer Service to:
  - Maintain records of data transfer activities, and
  - Ensure compliance with policies and legal requirements for the transmission of electronic data, including export controls, as specified in BMS-LGL-32.
- The transfer of physical media to a third party must follow the same policies, procedures, and guidelines as an electronic data transfer as specified in BMS-LGL-32. The physical media remains the property of Westinghouse and must be returned upon request or termination of employment or contract.
- When being transported, physical media must be protected in accordance with the classification of the information stored on the media. Requirements for the transportation of information are specified within BMS-LGL-32.
- Transfer of physical removable media must be reported to IT via the Service Desk.

1.8 Email and Instant Messaging

1.8.1 Westinghouse email and instant messaging use MUST be in accordance with the, **Westinghouse's Global Ethics Code**, **Westinghouse Standards of Conduct**, and **BMS-COM-4: Social Media Policy**.

1.8.2 In regards to Westinghouse email and instant messaging services, users MUST do the following:

- Use the following disclaimer for outgoing email:

  This email may contain proprietary information of the sending organization. Any unauthorized or improper disclosure, copying, distribution, or use of the contents of this email and attached document(s) is prohibited. The information contained in this email and attached document(s) is intended only for the personal and private use of the recipient(s) named above. If you have received this communication in error, please notify the sender immediately by email and delete the original email and attached document(s).

- Encrypt email that contains confidential and intellectual property in accordance with **BMS-LGL-32: Process for Marking and Handling Proprietary Information** and **BMS-LGL-28: The Classification, Reclassification and Release of Westinghouse Proprietary Information**.

- Comply with **BMS-LGL-32: Process for Marking and Handling Proprietary Information**, and **BMS-LGL-28: The Classification, Reclassification and Release of Westinghouse Proprietary Information** when sending confidential and proprietary information.
- Comply with local applicable export control regulations, as well as the requirements of the Westinghouse Export Control Manual when technical data or software is internationally disseminated.

1.8.3 In regards to Westinghouse email and instant messaging services, users are PROHIBITED from performing the following activities:

- Non-business related communication;

- Sending or forwarding unprofessional, threatening, defamatory, libelous obscene, offensive, or racist language, images, or audio;

- Sending or forwarding chain letters, spam, junk mail, sports-related, lottery, or gambling-related communication;

- Forging or attempting to forge messages or falsifying a person's identity;

- Sending internal or external email to a large target audience without prior approval from Westinghouse Communications;

- Manually or automatically forwarding email to a commercial email service (e.g., YahooMail, AOL, Gmail, HotMail) or another organization's email system;

- Forwarding or downloading Westinghouse email or to a personal (non-Westinghouse) device (e.g., mobile device, laptop, tablet);

- Storing Westinghouse email or Westinghouse email attachments to a personal (non-Westinghouse) device;

- Configuring email applications to automatically open emails and email attachments; and
- Using a scanned signature image in an email.

1.8.4 The use of email-enabled applications will be approved by the Information Technology Security Group and Director of Operations.

1.9 Remote Access & Teleworking

1.9.1 Authorized Westinghouse employees may utilize the benefits of Westinghouse remote access services to reach Westinghouse computer systems and computer data for which they have been granted access, subject to any restrictions required in accordance with Westinghouse export control considerations relevant to remote connection services and devices prior to approving any such access request.

1.9.2 Westinghouse's Chief Information Officer or Chief Information Security Officer Security may revoke, suspend, terminate, restrict, deny, or limit any remote access sought or previously granted with or without notice to affected employees, contingent labor personnel, customers, business partners, vendors, or other individuals or organizations at any time in order to protect Westinghouse computer data and to enforce Westinghouse computer security policies.

1.9.3 Methods for allowing remote access, as well as configuration settings, are established and maintained only by Westinghouse's Information Technology Department.

1.9.4 Only Westinghouse-configured workstations that meet Westinghouse's computer system configuration standards will be permitted remote access to Westinghouse's internal network. Westinghouse employees and contingent labor personnel working on behalf of Westinghouse and requiring remote access to Westinghouse computer systems and computer data will be issued Westinghouse-configured computers.

1.9.5 Any remote connection that is authorized in accordance with this policy will access the Internet only through Westinghouse's internal network. "Split tunnel" access, in which the remote workstation can simultaneously reach both the Internet and Westinghouse's internal network, is a serious security risk and therefore prohibited.

1.9.6 Exceptions for third parties, Westinghouse employees, or contingent labor personnel working on behalf of Westinghouse who are unable to use a Westinghouse computer because they work from a customer location that mandates use of the customer's workstations will only be permitted remote access:

- Upon written approval by Westinghouse's Chief Information Officer and the Chief Information Security Officer; and
- Upon verification that the customer's workstation(s) complies with Westinghouse's computer security standards.

1.9.7 Users must ensure their Westinghouse devices are physically secure when working remotely.

1.9.8 Remote access into restricted Westinghouse networks (e.g., isolated development infrastructures and plant control networks) is prohibited.

1.9.9 Third parties (such as vendors, customers, and other business partners) will remotely access Westinghouse computer systems using a dedicated network connection between the third party and Westinghouse provided that:

- Requests for network connections have been approved by the Chief Information Officer, Legal, and the Chief Information Security Officer; and
- A formal, written contractual arrangement has been entered into between Westinghouse and the third party.

1.9.10 Methods for allowing remote access between Westinghouse servers and any server outside of Westinghouse's internal network are available and supported by Westinghouse's Information Technology Department. Only Information Technology will establish remote connection services for servers, and only with the prior written approval of the Chief Information Officer and the Chief Information Security Officer. Any remote access between a Westinghouse server and a server that is outside of Westinghouse's internal network or any other unapproved installation of any type of remote access service or network gateway to the Internet is prohibited.

1.10 Internet Use

1.10.1 Westinghouse provided internet use must only be used for work-related activities and to fulfill work-related responsibilities.

1.10.2 Internet use must be in accordance with the **Westinghouse's Global Ethics Code**, **Westinghouse Standards of Conduct**, and **BMS-COM-4: Social Media Policy**.

1.10.3 Access to the internet is only permitted through internet access points that are approved and maintained by Information Technology.

1.10.4 Transmission of Westinghouse Proprietary Class 1, Westinghouse Proprietary Class 2, Personally Identifiable Information (PII), other data subject to regulatory control, and other intellectual property across the Internet, when performed in accordance with other applicable Westinghouse policies and procedures, must use approved encryption security controls.

1.10.5 Internet-facing Westinghouse web sites and Internet services (such as file sharing services) will only be established and maintained by Information Technology. Establishing an Internet-accessible web site from a Westinghouse computer system or through a third party web site hosting service without these approvals is prohibited.

1.10.6 The use of tools to circumvent, disable, modify, or otherwise alter any Westinghouse Internet security controls is strictly prohibited.

1.10.7 Westinghouse data is not allowed to be stored on external internet file servers without expressed written consent from the CIO, Legal, and Information Security.

1.10.8 Users are prohibited from posting Westinghouse intellectual property on the internet and must comply with **BMS-COM-4: Social Media Policy**.

1.11 Clear Desk and Clear Screen

1.11.1 Clear Desk

Printed copies of documents classified as Westinghouse Proprietary Class 1, or customer proprietary, must be stored in locked cabinets while not in use.

1.11.2 Clear Screen

While working on electronic documents classified as Westinghouse Proprietary Class 1, or customer proprietary, computers must be locked to prevent unauthorized access before leaving a computer workstation or terminal where this information is viewed.

1.12 Asset Management

1.12.1 Return of Assets

Upon termination of contract or employment, all IT assets, hardware, and software must be returned to Westinghouse. Employees are not permitted to retain any IT assets, including (but not limited to) personal computers, mobile telephones, tablet computers, removable media, or other devices capable of storing electronic data.

1.12.2 Computer Acceptable Use

1.12.2.1 Westinghouse computer systems must only be accessed by employees, contingent labor personnel, vendors, business partners, customers, and other third parties authorized in accordance with Westinghouse policies, procedures, and standards.

1.12.2.2 Third parties (e.g., vendors, customers, other business partners) must remotely access Westinghouse computer systems using a dedicated network connection between the third party and Westinghouse, provided that:

- Requests for network connections have been approved by the CIO, Legal, and the CISO.
- A formal, written contractual arrangement has been entered into between Westinghouse and the third party.

1.12.2.3 **Appropriate Use of Westinghouse Computer Systems**

All users of Westinghouse computer systems must protect company computers from illegal or damaging actions, either knowingly or unknowingly. The following are some examples of improper uses of Westinghouse computer systems, which are therefore prohibited:

- Using computer systems for purposes other than legitimate business. Computer systems may not be used for private commercial purposes, personal gain, partisan political purpose, other non-business related activity, or any unlawful activity.

- Intentionally or recklessly abusing or misusing computer systems so as to cause damage or system interruptions.

- Failing to use reasonable care to protect computer systems from loss or theft.

- Installing non-standard software on a computer system without first obtaining approval from IT as defined in **BMS-IS-46 Section 1.7.14**.

- Borrowing, lending, falsifying, or misusing a computer system or computer account.

- Allowing or facilitating unauthorized access to computer systems either inside or outside of Westinghouse.

- Obtaining credentials of other persons in order to use Westinghouse or Westinghouse-related computer systems, or impersonate another person on any Westinghouse computer system.

- Using computer systems or other electronic devices to harass or threaten other persons, or display, design, copy, store, draw, print, distribute, or publish obscene language, images, or graphics.

- Intercepting or attempting to intercept or otherwise monitor any communications not specifically intended for the assigned user without authorization from the Westinghouse CIO or CISO.

- Copying, reading, accessing, using, misappropriating, altering, publishing, or destroying computer files, output data, documents, or other files of another individual or the attempt to do so without the permission of the data owner.

- Making, distributing and/or using unauthorized duplicates of copyrighted material, including software applications, proprietary data, and IT resources. This includes sharing entertainment files (e.g., music, movies, video games) in violation of copyright law.

- Violating the terms and conditions of third party software license agreements for software distributed by Westinghouse by:

    - Giving, lending, selling, or leasing such media or software to others for their own use, or

    - Misusing it for personal use or on personal equipment

1.12.2.4 Appropriate Use of Westinghouse Customer Computer Systems and Computer Data

Employees, contingent labor personnel, vendors, business partners, customers, and other third parties:

- Must be aware of and comply with the customer's policies, procedures, and standards involving the use of customer computer systems and customer computer data at the customer's site.
- May not use a Westinghouse customer's computer systems nor access a customer's computer data unless the customer's management has provided Westinghouse management with written permission to do so.

References

The following documents are referenced in the Acceptable Use of Technology Policy:

- BMS-IS-46: Global Information Security Policy
- BMS-CI-2: BMS Policy and Procedure
- BMS-LGL-28: The Classification, Reclassification and Release of Westinghouse Proprietary Information
- Westinghouse's Global Ethics Code
- Westinghouse Standards of Conduct
- BMS-COM-4: Social Media Policy
- BMS-LGL-32: Process for Marking and Handling Proprietary Information
- BMS-IS-22 Westinghouse Computer Security Standard 232: *Encryption and Digital Certificates*
- Westinghouse Computer Security Standard 204: *Workstations, Laptops, and Mobile Devices*.
- *W2-9.17-102: Westinghouse Portable Media and Mobile Device (PMMD) Program Procedure*

Revision Summary

Revision	Date	Revision Description
0.0	10/03/2018	Initial Issue 10/31/2018

*** This record was final approved on 3/16/2021 9:51:17 AM. (This statement was added by the PRIME system upon its validation)

This page was added to the quality record by the PRIME system upon its validation and shall not be considered in the page numbering of this document.

Approval Information
Author Approval Mork Brian Feb-26-2021 09:36:12
Manager Approval Abram Michael Mar-16-2021 09:51:17

Files approved on Mar-16-2021

*** This record was final approved on 3/16/2021 9:51:17 AM. (This statement was added by the PRIME system upon its validation)